

# AML Rule Tuning: Applying Statistical and Risk-Based Approach to Achieve Higher Alert Efficiency

By: Umberto Lucchetti Junior, CAMS-FCI

**Table of Contents**

- 1. **Executive Summary** .....3
- 2. **Introduction** .....4
- 3. **Applying a Risk-Based Approach to the P Transaction Monitoring Scenerios** .5
  - a. **Implementation of a Population Group to the Transaction Monitoring Scenarios** .....7
  - b. **Implementation of a Suppression Logic to the Transaction Monitoring Process**.....9
- 4. **Qualitative and Quantitative Tuning of the Transaction monitoring scenarios**.....10
  - a. **Gap analysis** .....10
  - b. **Statistical Tuning of the Transaction Monitoring Scenerios** .....12
- 5. **Conclusion** .....15

## 1. Executive Summary

Recent fines against banks, such as, the ones applied to Standard Chartered Bank,<sup>1</sup> Saddle River Valley Bank<sup>2</sup> and HSBC Bank,<sup>3</sup> for failing to detect suspicious activity and therefore failing to comply with the transaction monitoring portion of the compliance program, have demonstrated the importance of having a sound anti-money laundering (AML) compliance program. In order to maintain AML detection scenarios current with best market practices, rule tuning exercises have become an ever-increasing important task to perform at a financial institution. The methodologies to tune AML detections scenarios are also becoming more complex with heightened expectations from regulators. The tuning needs to be constant, that is, continuously applied over time to identify potential new risks or new typologies not covered by the current process in place. Likewise the application of a risk-based approach to the transaction monitoring process should also be taken into consideration by banks since it helps to focus the efforts and resources of staff on what poses a higher money laundering risk for the institution. This tuning will directly benefit the financial intelligence unit (FIU) and consequently the financial crime investigators who will have more productive alerts to review, having more time to investigate the potential suspicious alerts, therefore, improving the transaction monitoring process as a whole.

Based on that, this white paper provides an overview of the importance of the AML rule tuning and the application of the risk-based approach to the transaction monitoring process, defining and giving examples on how to implement and perform these two important processes to the transaction monitoring scenarios of a bank.

---

<sup>1</sup> From the New York State Department of Financial Services Press Release of August 19, 2014.

<http://www.dfs.ny.gov/about/press2014/pr1408191.htm>.

<sup>2</sup> From FinCEN Assessment of Civil Money Penalty of September 24, 2013.

[http://www.fincen.gov/pdf/SRVB\\_Assessment\\_092413.pdf](http://www.fincen.gov/pdf/SRVB_Assessment_092413.pdf)

<sup>3</sup> From FinCEN Assessment of Civil Money Penalty of December 10, 2012.

[http://www.fincen.gov/news\\_room/ea/files/HSBC\\_ASSESSMENT.pdf](http://www.fincen.gov/news_room/ea/files/HSBC_ASSESSMENT.pdf)

## 2. Introduction

The identification and reporting of suspicious activity is one of the most important processes of an institution's compliance program. Within the suspicious activity reporting, the transaction monitoring process plays an important role on the identification of unusual activity. According to the Federal Financial Institutions Examination Council (FFIEC) manual,<sup>4</sup> "the sophistication of monitoring systems should be dictated by the bank's risk profile, with particular emphasis on the composition of higher-risk products, services, customers, entities, and jurisdictions."<sup>5</sup> The basis for the development of the monitoring systems should be on the Bank Secrecy Act/anti-money laundering (BSA/AML) risk assessment, which is a mandatory assessment to be conducted by banks as part of the compliance program. This assessment highlights areas of a bank's risk, and exposes any potential gaps in controls that should be implemented to mitigate these risks. Most of the banks rely on automated systems to identify unusual activity and generate alerts. Using the same concept, the sophistication and complexity of this system should be based on the bank's risk profile.

Banks are subject to findings by examiners on the suspicious activity reporting portion of the compliance program because the AML system is not properly tuned in accordance with the bank's risk profile. Outdated rules oftentimes cause an inefficient allocation of resources as analysts have a high number of false positive alerts to review. A high number of false positive alerts present a bank's AML program with a risk where the analysts may not have the sufficient time to handle all alerts with a high quality review, where potentially suspicious activity may be overlooked.

---

<sup>4</sup> The Federal Financial Institutions Examination Council (FFIEC) Bank Secrecy Act (BSA)/Anti-Money Laundering (AML) Examination Manual provides guidance to examiners for carrying out BSA/AML and Office of Foreign Assets Control (OFAC) examinations. An effective BSA/AML Compliance Program requires sound risk management; therefore, the manual also provides guidance on identifying and controlling risks associated with money laundering and terrorist financing. The manual contains an overview of BSA/AML Compliance Program requirements, BSA/AML risks and risk management expectations, industry sound practices, and examination procedures.

<sup>5</sup> From the FFIEC Manual, Suspicious Activity Reporting Section:

(<http://www.occ.treas.gov/publications/publications-by-type/other-publications-reports/ffiec-bsa-aml-examination-manual.pdf>)

As per IPSA International<sup>6</sup> “one of the biggest issues facing investigators is the generation of a 'false positive.' A false positive is not an accurate alert and should not be flagged for investigation. This results in a lower productivity for the investigator and increases the likelihood of a ‘true positive’ being spotted.”<sup>7</sup>

One of the potential solutions for this lack of proper tuning of the transaction monitoring process is the application of a risk-based approach and the qualitative and quantitative tuning of the transaction monitoring scenarios in order to achieve a higher alert efficiency, therefore, improving the suspicious activity reporting process as a whole.

### **3. Applying a Risk-Based Approach to the P Transaction Monitoring Scenarios**

According to the Wolfsberg Group<sup>8</sup> guidance, “financial institutions should design and implement appropriate measures and controls to mitigate potential money laundering risks of those customers that are determined to be higher risk as the result of the institution’s risk assessment process. These measures and controls may include increased monitoring of transactions.”<sup>9</sup>

Yet as per the Financial Action Task Force (FATF),<sup>10</sup> “a Risk Based Approach to Anti Money Laundering (AML)/Combating the Financing of Terrorism (CFT) means that countries, competent authorities and financial institutions, are expected to identify, assess and understand the Money Laundering/Terrorism Financing risks to which

---

<sup>6</sup> IPSA is an international consulting firm that provides services on the AML area.

<sup>7</sup> From IPSA website: <http://www.ipsaintl.com/Articles/trade-finance-aml-monitoring.html>.

<sup>8</sup> The Wolfsberg Group is an association of eleven global banks, which aims to develop financial services industry standards, and related products, for Know Your Customer, Anti-Money Laundering and Counter Terrorist Financing policies. The Wolfsberg Group consists of the following leading international financial institutions: Banco Santander, Banco of Tokyo Mitsubishi-UFG, Barclays, Citigroup, Credit Suisse, Deutsche Bank, Goldman Sachs, HSBC, JP Morgan Chase, Societe Generale and UBS.

<sup>9</sup> From the Wolfsberg Statement, Guidance on a Risk Based Approach for Managing Money Laundering Risks: [http://www.wolfsberg-principles.com/pdf/standards/Wolfsberg\\_RBA\\_Guidance\\_\(2006\).pdf](http://www.wolfsberg-principles.com/pdf/standards/Wolfsberg_RBA_Guidance_(2006).pdf).

<sup>10</sup> The Financial Action Task Force (FATF) is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction.

they are exposed and take AML/CFT measures commensurate to those risks in order to mitigate them effectively.”<sup>11</sup>

The application of the risk-based approach starts, ideally, on the BSA/AML risk assessment where the bank will understand, identify and assess the money laundering risks posed by the products and services offered, the customers’ risk profile, the risks posed by the geographies the bank has business with, among other risks. Based on the risks identified, the institution will implement controls to mitigate these risks. Here is where the risk-based approach comes into play. The institution will implement a closer monitoring to higher risk customers, products and geographies.

The FATF confirms that this exercise should be performed and described on the BSA/AML risk assessment: “when assessing Money Laundering/Terrorist Financing risks, countries, competent authorities, and financial institutions should analyze and seek to understand how the Money Laundering/Terrorist Financing risks they identify affect them; the risk assessment therefore provides the basis for the risk-sensitive application of Anti-Money Laundering/Combating the Financing of Terrorism measures.”<sup>12</sup>

The application of the risk-based approach to the transaction monitoring scenarios can be achieved by taking some measures within the transaction monitoring system, such as, incorporating the customers’ and products’ risk levels into the rules suite and implementing a suppression of repetitive alerts closed as non-issue. The final goal of these measures is to have less false positive alerts for low risk customers and consequently more time to review potential positive alerts.

---

<sup>11</sup> From the FATF Guidance for a Risk Based Approach to the Banking Sector:  
<http://www.fatf-gafi.org/media/fatf/documents/reports/Risk-Based-Approach-Banking-Sector.pdf>.

<sup>12</sup> From the FATF Guidance for a Risk Based Approach to the Banking Sector:  
<http://www.fatf-gafi.org/media/fatf/documents/reports/Risk-Based-Approach-Banking-Sector.pdf>.

Considering that nowadays the institutions are continually trying to achieve efficiency in terms of costs and resources the application of the risk-based approach to the transaction monitoring scenarios can, not only improve the quality and effectiveness of the transaction monitoring process, but also play an important role on the cost saving process because it will help institutions to save time and resources and focus the efforts on what is riskier for the bank.

However, it must be clear that this risk-based approach does not exempt the financial institutions to implement controls to mitigate low risks identified in the risk assessment, as explained by FATF: “A risk based approach does not exempt countries, competent authorities and financial institutions from mitigating Money Laundering/Terrorist Financing risks where these risks are assessed as low.”<sup>13</sup> Low risks must be mitigated but on a lighter way if compared to higher risks.

The two measures mentioned above, the population group and the suppression logic are described below.

#### **a. Implementation of a Population Group to the Transaction Monitoring Scenarios**

Most AML rule scenarios focus solely on the activity of a client, not incorporating any risk elements of the bank’s know your customer (KYC) program and other client-specific risk elements such as product risk. In order to apply the risk-based approach to AML monitoring, it is essential to introduce such risk elements as additional parameters to the AML detection scenarios.

The population group consists on the incorporation of certain money laundering risks identified in the BSA/AML risk assessment to the transaction monitoring scenarios,

---

<sup>13</sup> From the FATF Guidance for a Risk Based Approach to the Banking Sector:  
<http://www.fatf-gafi.org/media/fatf/documents/reports/Risk-Based-Approach-Banking-Sector.pdf>.

which can be translated as the application of a risk-based approach to the transaction monitoring rules.

For the purposes of this exercise, only the client’s risk level and product will be considered. The exercise will be based on a bank that offers three different types of products to their customers. These products were assessed in the risk assessment as follows: Product 1 – Low Risk; Product 2 – Medium Risk and; Product 3 – High Risk. The customers are classified as low, medium and high risk. These two parameters, products risk and customers risk will be combined and plotted in a heat map in order to create three different levels of population group: low, medium and high. The heat map created follows:

		Product Risk		
		Product 1 Low	Product 2 Medium	Product 3 High
Customer Risk				
	High	Orange	Red	Red
	Medium	Green	Orange	Red
	Low	Green	Green	Orange

The result of the combination of risks is: Population Group 1 – Low Risk (green cells), Population Group 2 – Medium Risk (orange cells) and Population Group 3 – High Risk (red cells). If a customer trades more than one product the riskier one will be considered for the identification of the population group this customer will fall into.

The population groups will then be applied to the transaction monitoring scenarios so that different thresholds will be defined for each population group category. Taking into considering the risk-based approach, higher thresholds will be applied to the low-risk population group and lower thresholds will be applied to the high-risk population group. Using this methodology, the system will generate fewer alerts for the low-risk

customers and products saving time and resources to be allocated on the higher risk customers and products.

Another layer that could be introduced to the population group, for example, could be the separation of customers by its size since larger customers tend to conduct transactions of higher amounts and volume than smaller customers. In this sense, another layer of the population group would be created to separate small, medium and big customers and apply different thresholds for them.

#### **b. Implementation of a Suppression Logic to the Transaction Monitoring Process**

Another important process that can be implemented to contribute to the risk-based approach is a suppression of alerts consecutively closed as a non-issue, which were previously investigated and deemed to be not suspicious.

Depending on a bank's risk tolerance and profile, this suppression logic could be implemented only for a subset of the client populations such as only for low and medium risk population groups.

The logic consists in the suppression of alerts, generated for a specific customer and rule. In order for an alert to be suppressed, a specific client and rule would have had to be deemed false positives over several monthly alert generations. The following is an example of how the suppression logic may be applied in an automated AML system: for the low-risk population group an alert would be suppressed after six prior alerts closed as non-issue and for the medium risk population group after nine prior alerts closed as non-issue. No suppression would be activated for high-risk population group as per the risk-based approach taken. These alerts would not be suppressed forever though, they would be generated again after they have been suppressed three times, that is, in the fourth time.

In order to lessen the risk of not capturing potential suspicious activity caused by the suppression of these alerts, a review of the customer's activity of the previous six months for all alerts must be in place, which is a common and best practice within the industry.

#### **4. Qualitative and Quantitative Tuning of the Transaction monitoring scenarios**

To assure that all money laundering and terrorist financing risks posed by the customer's base and products and services offered are covered and to achieve a higher alert efficiency, two key exercises should be performed to fulfill these goals: a gap analysis and a statistical tuning of the transaction monitoring scenarios.

##### **a. Gap analysis**

According to Crowe Horwarth's<sup>14</sup> guidance on Model Tuning and Optimization, "A gap analysis, also known as a coverage assessment, analyzes known risk factors within each AML model to determine if the risk is adequately mitigated or controlled. If there are gaps in coverage, the model owner should establish a remediation plan to address those gaps. When developing the universe of risk areas to consider, the bank can refer to the Federal Financial Institutions Examination Council Bank Secrecy Act/Anti-Money Laundering Examination Manual (FFIEC) and the bank's own risk assessment. The bank should also consider the industry and regulatory environment as well as known money-laundering trends".<sup>15</sup>

A secondary goal of the gap analysis is to identify products that are not being monitored or even redundancies on the transaction monitoring scenarios in place.

---

<sup>14</sup> Crowe Horwath LLP is one of the largest public accounting and consulting firms in the United States.

<sup>15</sup> From Crowe Horwarth's paper on Model Tuning and Optimization:

[http://www.crowehorwath.com/folio-pdf/RISK13910\\_AMLModelTuningArticle\\_lo.pdf](http://www.crowehorwath.com/folio-pdf/RISK13910_AMLModelTuningArticle_lo.pdf).

The gap analysis is a continuous exercise that should be preferably performed in conjunction with the BSA/AML risk assessment where the risks are identified and should be updated whenever the risk assessment is updated in order to identify new risks or new typologies not covered by the scenarios in place.

The first step to be taken on the gap analysis is to make sure that all products and services that pose any money laundering or terrorist financing risks are being monitored either manually or by the automated surveillance system. In order to complete this exercise, a list of approved products must be obtained and a reconciliation be performed with the current products monitored in order to identify potential gaps. Products that do not pose any money laundering or terrorist financing will not be monitored, but a rationale must be clearly described within the document for examination purposes.

The second step on the gap analysis is to corroborate that all risks posed by the products and services offered, customers risk profile and geography risk are covered by the transaction monitoring scenarios in place. For purposes of this white paper we are going to give examples of a bank that offers cash accounts and loans to its corporate customers.

The exercise can be applied as follows. The list below shows only some of the money laundering risks associated to the products offered. There are many other risks that are not listed in the table below.

<b>Product</b>	<b>Risks</b>	<b>Rule in Place to Cover Risk (Y/N)</b>
Cash Account	Structuring	Y
	Round Dollar Transactions	Y
	Wires to/from High-Risk Jurisdictions	N
	High Amount Transactions	Y
	Activity Profile Deviation	N
	Dormant Accounts	Y

Loans	Early Termination	N
	Multiple Payments	Y
	Third-Party Payments	N

According to the exercise illustrated above, the bank identified weaknesses on the transaction monitoring process; therefore, will need to implement new scenarios to cover the existent gaps, that is, the identified risks for which there are no rules in place to mitigate them.

**b. Statistical Tuning of the Transaction Monitoring Scenerios**

Another component of the transaction monitoring scenarios tuning is the application of statistical tests to the rules' thresholds with the final goal to try to determine the best possible thresholds, which will result in the decrease of false positive alerts contributing to the improvement of the alert efficiency. According to Protiviti's<sup>16</sup> paper "Avoiding Buyer's Remorse with AML Monitoring Software," "a high percentage of alerts escalated to cases are a sign a rule is efficient and effective. Cases indicate there is potentially suspicious activity and require additional review by the monitoring team before they are cleared or escalated again for SAR filings. Financial institutions should review any rules that have low alert-to-case ratios to understand whether parameters should be adjusted to lower the "false positives" (the number of alerts cleared without escalation)."<sup>17</sup> The alert-to-case ratio will vary among institutions based on the services and products offered and will also vary among transaction monitoring rules based on the logic of each rule. Although there is no standard ratio to be pursued, the statistical tuning must target the highest possible ratio for each rule.

---

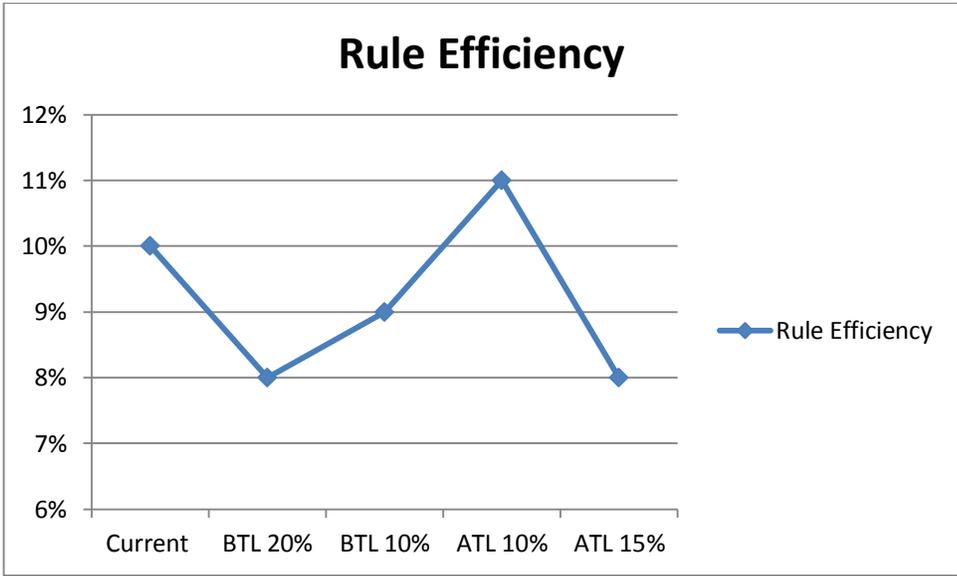
<sup>16</sup> Protiviti is a global consulting firm that helps companies solve problems in finance, technology, operations, governance, risk and internal audit.

<sup>17</sup> From Protiviti's paper Avoiding Buyer's Remorse with AML Monitoring Software <http://www.protiviti.com/en-US/Documents/White-Papers/Risk-Solutions/AML-Transaction-Monitoring-Systems-Protiviti.pdf>

The statistical tuning can be performed by applying statistical methods known as above-the-line (ATL) and below-the-line (BTL) testing approach to validate and tune the rules' thresholds and parameters. ATL and BTL testing consists in increasing and decreasing rules' thresholds in order to try to achieve the best possible threshold and parameters taking into consideration the current rule efficiency ratio and the ratio obtained by the tests performed. As a market standard it is customary to start the rule tuning process based on 10 percent above and below the current thresholds. This percentage can be increased or decreased, for instance to 20 percent or 5 percent, respectively, on both sides, above and below, if no satisfactory results were obtained with the initial percentage applied. To initiate the tests, the thresholds are then changed on the system's testing environment and alerts are generated for at least the transactions of the previous six months.

The next step of the tuning process is the performance of a pseudo investigation only on the differential alerts generated for the new thresholds lowered in order to determine if they are good or bad alerts. Since the exercise is applied on past data, for which alerts have already been generated and reviewed, it will not be necessary to review the same alerts generated, therefore, only the differential alerts will be reviewed. Also, it is important and necessary to determine if no good alerts were missed by increasing the thresholds. Good alerts can be defined as alerts that turned into cases or alerts that led to SARs. For the purposes of this exercise we are going to use alerts that turned into cases. Also for the purposes of this exercise, rule efficiency is defined by how many alerts converted into case in comparison to the total number of alerts generated for that rule. A target rule efficiency ratio should be defined by the institution before starting the tuning. Below is an example of a statistical tuning on a plain vanilla rule that captures activity above \$1 million, the only parameter of the rule. Below are the hypothetical results of the ATL and BTL tests as well as the pseudo investigations on the alerts generated for the exercise.

<b>Metrics</b>	<b>Current Threshold – 1 Million</b>	<b>BTL 20% 800,000</b>	<b>BTL 10% - 900,000</b>	<b>ATL 10% 1.1 Million</b>	<b>ATL 15% 1.15 Million</b>
# of Alerts	100	130	110	90	80
Cases Created	10	11	10	10	7
Rule Efficiency	10%	8%	9%	11%	8%



Based on the outcome of the tuning exercise above, the change that resulted in the higher rule efficiency ratio was the ATL 10 percent. Although no new cases were identified, the change resulted in less alerts increasing the efficiency ratio. The BTL 10 percent also resulted in no new cases identified but increased the number of alerts decreasing then the rule efficiency ratio. On the BTL 20 percent, one new case was identified, but the number of alerts increased considerably, decreasing the rule efficiency even more. The ATL 15 percent also decreased the number of alerts, but also decreased the number of cases created, that is, good alerts were missed by this change. Based on the results obtained, no further changes are necessary on both sides since the ATL side was observed some good alerts were missed and on the BTL side the change on the cases was not high when compared to the increase in

the number of alerts. The threshold on the production environment will then be increased by 10 percent, as a result of the statistical tuning.

## **5. Conclusion**

As illustrated in this white paper, the risk-based approach and the tuning of the transaction monitoring scenarios are an important part of the compliance program because they can improve the efficiency of the alert review process as well as cover potential existent gaps on the transaction monitoring process. Furthermore, these two exercises help financial institutions, the FIU and the financial crime investigators to focus on the riskier customers and products as required by the regulations in place. Therefore, these two exercises should be applied on a continuous basis so that the process will continue to enhance over time. At a minimum, these exercises should be performed on an annual basis in conjunction with the bank's annual risk assessment.